Money talks money laundering choices of organized crime offenders in a digital age

Kruisbergen, E. W.; Leukfeldt, E. R.; Kleemans, E. R.; Roks, R. A.

published in
JOURNAL OF CRIME & JUSTICE
2019

DOI (link to publisher)
10.1080/0735648X.2019.1692420

document version
Publisher's PDF, also known as Version of record

Journal of Crime and Justice

ISSN: 0735-648X (Print) 2158-9119 (Online) Journal homepage: https://www.tandfonline.com/loi/rjcj20

Money talks *money laundering choices of organized crime offenders in a digital age*

E.W. Kruisbergen, E.R. Leukfeldt, E.R. Kleemans & R.A. Roks

To cite this article: E.W. Kruisbergen, E.R. Leukfeldt, E.R. Kleemans & R.A. Roks (2019) Money talks *money laundering choices of organized crime offenders in a digital age*, Journal of Crime and Justice, 42:5, 569-581, DOI: 10.1080/0735648X.2019.1692420

To link to this article: https://doi.org/10.1080/0735648X.2019.1692420

JOURNAL OF CRIME AND JUSTICE
2019, VOL. 42, NO. 5, 569–581
https://doi.org/10.1080/0735648X.2019.1692420

Routledge
Taylor & Francis Group

Money talks *money laundering choices of organized crime offenders in a digital age*

E.W. Kruisbergen[a], E.R. Leukfeldt[b], E.R. Kleemans[c] and R.A. Roks[d]

[a]Department of Crime, Law Enforcement and Sanctions, Research and Documentation Centre (WODC), the Dutch Ministry of Justice and Security, Den Haag, The Netherlands; [b]Netherlands Institute for the Study of Crime and Law Enforcement (NSCR), Amsterdam / Cybersecurity and SMEs research group, the Hague University of Applied Sciences, The Hague, Amsterdam, The Netherlands; [c]VU School of Criminology, Faculty of Law, Vrije Universiteit Amsterdam, the Netherlands, Amsterdam, The Netherlands; [d]Department of Criminology, Erasmus School of Law, Erasmus University of Rotterdam, Rotterdam, The Netherlands

ABSTRACT

In this explorative study we provide empirical insight into how organized crime offenders use IT to launder their money. Our empirical data consist of 30 large-scale criminal investigations into organized crime. These cases are part of the most recent, fifth data sweep of the Dutch Organized Crime Monitor (DOCM). We do not focus on cybercrime alone. Instead, we explore the financial aspects of criminal operations in a broad range of types of organized crime, i.e. from 'traditional' types of organized crime, such as offline drug smuggling, to cybercrime. Regarding the spending of criminal proceeds (consumption and investment), the analyses show several similarities and no major differences between traditional crime and cybercrime. When it comes to concealing criminal earnings (money laundering), we do see important differences. Financial innovation, such as the use of cryptocurrencies, seems to be limited to cases of IT-related crime. One of the most striking similarities between cybercrime and traditional crime is the offenders' preference for cash. In the analysed cases, malware and phishing offenders as well as online drug traffickers change their digital currencies for cash, at least in part.

KEYWORDS

Cybercrime; Organized Crime; Money Laundering

Organized crime and IT: new theoretical and empirical questions

The massive use of the internet, and more generally the effect of IT (information technology) on all segments of society, entails new opportunities for organized crime. The use of IT in relation to organized crime raises several interesting questions. This is especially true when new forms of crime such as cybercrime, or the use of new technology in traditional organized crime, are linked to existing knowledge, concepts, and theories in the field of organized crime. For example, it is worthwhile to consider what the use of IT means for the way in which organized crime groups emerge and develop. Has, for example, the internet diminished the importance of real-life social capital for the participation in organised crime (Lavorgna 2013; Przepiorka, Norbutas, and Corten 2017; Töttel, Bulanova-Hristova, and Flach 2016, 28–30; Leukfeldt 2017)? Another interesting issue regards the role of IT in the logistics of organized crime. Any form of organized crime can be described as a logistical process in which a number of necessary steps must be taken (Cornish and Clarke 2002). These steps may include, for example, production/purchase of drugs, transport and

CONTACT E.W. kruisbergen e.w.kruisbergen@minvenj.nl Research and Documentation Centre, Ministry of Justice and Security, PO Box 20301, Den Haag 2500 EH, The Netherlands

storage, crossing border controls, and sales. In what way do criminals use IT to improve the logistical process and does the use of IT potentially lead to new logistical bottlenecks?

Handling money flows is a specific type of bottleneck for every successful offender. Organized crime is motivated – at least in part – by financial gain. However, criminal earnings bring certain risks, especially if your criminal operations are successful and generate a lot of money. Criminal earnings *and* the spending of those earnings may raise suspicion, which in turn could lead to arrest and confiscation of your assets. How and to what extent do offenders use IT-facilitated possibilities, such as bitcoin, to launder their money?

Until now, there is only a limited amount of empirical research into how criminals use these options and what consequences the use of IT has for how criminals operate (Leukfeldt 2017; see also Lagazio, Sherif, and Cushman 2014). A number of studies have recently been published. Odinot et al. (2017) and Bulanova-Hristova et al. (2016) analysed criminal investigations in the field of cybercrime. These studies explored on the modus operandi, structures and profiles of individual offenders in these networks. Furthermore, the authors focussed on challenges and obstacles of law enforcement agencies have to deal with during investigations. The authors conclude, amongst other things, that the Internet functions as a tool to increase the efficiency of crime scripts and provides for new business opportunities. Leukfeldt et al. also conducted empirical research into cybercrime, focusing in particular on the processes of origin and growth and modi operandi of cybercriminal networks (Leukfeldt, Kleemans, and Stol 2017a, 2017b, 2017c; Leukfeldt, Lavorgna, and Kleemans 2017d). These studies show the importance of online and offline social contact for the functioning of cybercriminal networks. Finally, Custers, Pool, and Cornelisse (2018) looked into how money is laundered in cybercrime cases.

Our study provides empirical insight into how organized crime groups use IT to handle their money flows. We build on the work of these and other researchers by both broadening and deepening their work. Similar to Custers, Pool, and Cornelisse (2018), we focus on criminal money flows. However, whereas they focused on money laundering in several cybercrime cases, we explore the use of IT in relation to money flows in a broad range of types of organized crime, i.e. from 'traditional' types of organized crime, such as offline drug smuggling, to cybercrime. After all, the potential use of IT facilitated possibilities for money laundering purposes is not limited to cases of cybercrime. Offenders involved in offline drug trafficking operations may convert their cash revenues into cryptocurrencies and prepaid cards to obscure their money flows, for example. Are these possibilities actually used by offenders in traditional, offline types of organized crime? Furthermore, we do not only look into the laundering of criminal earnings, but also explore the spending of those earnings. We address the following research question: *How and to what extent do offenders use IT-facilitated possibilities to handle their money flows?* The empirical data we use consist of the 30 cases that were analysed in the fifth and most recent data sweep of the Dutch Organized Crime Monitor. The fifth wave of this ongoing research project is the first to include cases of cybercrime. This allows us to analyse the use of IT in relation to criminal money flows in a broad range of types of organized crime, including both offline and online organized crime.

In the following section (section 2), we focus on the existing literature on money laundering choices of organized crime offenders. In section 3, the research methods and empirical data are explained. In Section 4, we present the results of the empirical analyses. In Section 5, we summarise the empirical results, discuss the theoretical implications, and provide suggestions for future research.

Prior research

Money laundering literature might be classified into three groups. First, several authors tried to assess the size of financial flows involved in money laundering. Scholars such as Walker (1995), Schneider (2010), Barone and Masciandaro (2011, 116–118), and Unger et al. (2006) have produced a wide range of estimations. Other criticize these attempts to measure the amount of money laundered. Because of a lack of solid methodology and valid data, credible results are

simply not possible (Reuter 2013). Therefore, according to critics, assessments result in nothing more than 'speculative guesstimates' (Levi 2012, 610), although these guesstimates have become 'facts by repetition' because they are cited so frequently (Levi and Reuter 2009, 362). Second, there is an abundance of articles and books in which policy measures against money laundering are critically reviewed (Levi and Reuter 2009, 359). The third category consists of empirical studies on what offenders actually do with their money, and what type of money laundering methods they use. This type of empirical research is relatively scarce (Kruisbergen, Kleemans, and Kouwenberg 2015, 240; Fernández Steinko 2012, 909; Levi 2012; Verhage 2011, 172). This applies even more for cybercrime than for cases of traditional (organized) crime (see also Werner and Korsell 2016).

Criminal earnings can be reinvested in criminal activities, they can be consumed, and, if there is any money left, criminal earnings can also be invested in legal economy. From a policy perspective, these investments are the most interesting category of spending. The perceived threat of criminals investing huge sums of money and, as a result, gaining influence in economic, social, and political spheres, is an important driving force behind anti-money laundering measures (see for a review, e.g. Levi and Reuter 2009). Regarding the investments in legal economy, there is a modest number of empirical studies. Prior research showed organized crime offenders predominantly invest in their country of origin or in their country of residence (Kruisbergen, Kleemans, and Kouwenberg 2015, 250; Webb and Burrows 2009, 27; Van Duyne and Levi 2005; Suendorf 2001). Furthermore, many offenders invest in real estate, residences in particular (Kruisbergen, Kleemans, and Kouwenberg 2015, 243–244; Kleemans et al. 2002; Webb and Burrows 2009, 27; Matrix Knowledge Group 2007, 39; Fernández Steinko 2012; Malm and Bichler 2013; Van Duyne and Soudijn 2010, 271; Van Duyne 2003, 98–101; Schneider 2004; Transcrime 2013; Petrunov 2011, 177–178). Another type of assets often found in the portfolio of organized crime offenders concerns companies, i.e. wholesale/retail companies, hotels, bars and restaurants, transportation companies, and brothels. One might say that offenders predominantly invest in goods and companies that they are familiar with from everyday life. In many of these companies, offenders are somehow personally involved, i.e. companies are directly or indirectly controlled by an offender, are used for criminal purposes, and/or actual economic activity takes place within the company on behalf of the offender (Kruisbergen, Kleemans, and Kouwenberg 2015; see also Bruinsma 1996; Suendorf 2001; Schneider 2004; Transcrime 2013; Matrix Knowledge Group 2007; Petrunov 2011). Purely financial assets, on the other hand, i.e. bonds, options, and stocks in companies in which offenders are not personally involved (such as stocks in companies noted on the stock exchange), are far less often found (Kruisbergen, Kleemans, and Kouwenberg 2015).

Other studies focus on the methods offenders use to hide the criminal origin of their assets. The Dutch police periodically publishes research reports on money laundering in which statistics, interviews, and case files are analysed. Soudijn (2018) analysed four so-called Crime Pattern Analyses (CPAs), covering a time span of twelve years. Continuity in money laundering methods appears to be far more prominent than change. The results show that well-known methods of money laundering keep returning. These are the methods of loanback, fictitious turnover in legal companies, fictitious gambling profits, and trade based money laundering. The most prominent returning theme in the four CPAs is the important role of cash (see also Custers, Pool, and Cornelisse 2018; Europol 2015; Kruisbergen, Van de Bunt, and Kleemans 2012). Some changes in methods of money laundering did take place. These are for an important part technology driven, such as the (rise in the) use of bitcoin and prepaid cards, mostly for relatively small amounts. Fundamental, large-scale changes in the field of money laundering, however, did not seem to occur (Soudijn 2018).

Empirical studies on money laundering in cybercrime case are (even) scarcer (see also Werner and Korsell 2016). Custers, Pool, and Cornelisse (2018) explored the money laundering methods used by offenders in cases of banking malware. They identified two models for laundering the profits of banking malware. The first model involved the use of money mules and a quick cash-out. In that model the money is transferred from the victim's bank account to the money mule's bank account. The money mule subsequently withdraws the money via an ATM. The second model involves the

direct spending of the profits in the online banking environment. In the section 'Empirical results', we will compare our own results with the main results of (some of) the studies mentioned above.

Current study

Our empirical data consist of large-scale criminal investigations into organized crime. These cases are part of the Dutch Organized Crime Monitor (DOCM). The DOCM is an ongoing research project into the nature of organized crime in the Netherlands. The main sources of information for the DOCM are closed Dutch criminal investigations into criminal groups. In five data sweeps, 180 large-scale cases of organized crime have been analysed. As each case focuses on a criminal network, the cases include many suspects (up to 49 per case in the most recent data sweep). Together the 180 case reports contain information on many hundreds of suspects.

Case studies are selected following a survey of criminal investigations of the police force and special investigative policing units. The selection is not random. In fact, a random sample is inconceivable in organized crime research, as police priorities provide the basis for any sample. We, therefore, opt for a strategic sample incorporating the heterogeneity of criminal activities and offenders. Richness of information is an important selection criterion. Each case study starts with a structured interview with a police officer and/or public prosecutor. Subsequently, the files are analysed and a systematic case report is written. The police files contain the results of all police activities that were deployed in a case, such as wiretapping, monitoring of internet traffic, undercover policing, interrogations of suspects, confiscation of goods, and financial information. Systematic case reports are written using an extensive checklist. The checklist elaborates upon: the composition of the group and how offenders cooperate; the illegal activities they participate in and the modus operandi; the interaction with the licit as well as the criminal environment; the criminal earnings and how these earnings are spent; the criminal investigation itself; the criminal court case; and opportunities for prevention.

For this article, we used the 30 cases that were analysed in the fifth and most recent data sweep.[1] The results of the analyses were published in a Dutch research report. A draft of the report was reviewed by specialists within the police, who checked if the main research findings stood up to their knowledge of most recent developments (for more information, see Kruisbergen et al. 2018). To gain insight into the financial aspects of these cases – which is the purpose of this article, we analysed all 30 case reports, focusing on spending of criminal earnings (i.e. consumption and investments) and laundering of criminal earnings (i.e. rudimentary laundering methods involving cash money, more complex laundering methods such as faking legal profit or salary, and new types of money laundering involving cryptocurrencies and prepaid cards, for example).

The 30 cases cover various types of organized crime, such as various types of drug trafficking, illegal arms trade, human trafficking, fraud and money laundering, and cybercrime. We distinguish between four categories of cases, depending on the role IT plays. The first category comprises 23 cases of *traditional organized crime*; in other words, cases without a strong IT component. These include cases of offline drug trafficking (cases 158, 159, 161–164, 167, 169–172, 175, and 176)[2], human smuggling/trafficking (case 160), money laundering (cases 157, 166, 168, 177, 178, and 180), and other/combined crimes (cases 165, 174 and 179).

The second category concerns three cases of *traditional organized crime* with IT as an important innovative element in the modus operandi. One of these cases concerns an offender group manipulating the handling of incoming containers through a hack in the network of a port terminal (case 151). A second case concerns people involved in a dark web market through which drugs are traded, among other things (case 152). The final case revolves around a modern variant of money laundering. It entails bitcoin exchangers helping their customers exchange bitcoins for cash anonymously. Available information indicated that these customers earned their bitcoins through online drug trafficking (case 173).

The third category comprises two cases of *organized low-tech cybercrime*. One case concerns a variant of 'skimming' (also known as 'shimming'): the magnetic strip of a bank card is not copied;

instead, the data traffic between the so-called EMV chip on the card and the terminal in which it is used is intercepted (case 154). A second case concerns phishing operations, in which criminals seek to obtain people's online banking credentials, among other things (case 156).

Finally, the fourth category includes two cases of *organized high-tech cybercrime*. Both cases focus on banking malware, i.e. criminals manipulate payments made via internet banking through malicious software (cases 153 and 155).

Therefore, our data include 23 cases of traditional organized and 7 cases of IT-related crime or cybercrime. The fifth wave of the Dutch Organized Crime Monitor is the first to include cases of cybercrime. At the time selection of cases for the fifth wave took place, 2014/2015, there were hardly any more cybercrime cases with sufficient size and scope fitting our criteria: cases of organized cybercrime in which the criminal investigation had been closed.[3] At that time, cybercrime was still a relatively new phenomenon for criminal investigators. Furthermore, many cybercrimes are committed by offenders residing abroad, which hampers the successful investigation and, especially, prosecution of offenders. Finally, the police, public prosecution office and other authorities involved, often choose to disrupt online criminal activities instead of deploying a full-fledged criminal investigation and prosecution (see also Schuppers et al. 2016).

Empirical results

Spending of criminal earnings

In general, the financial position of organized crime offenders is far from transparent, for obvious reasons. The 30 cases we analysed, however, offer valuable insights, due to the exclusive powers the police deploy during criminal investigations. How do offenders spend their money? We will briefly discuss consumption as well as investments. Several cases of offline as well as cases of online organized crime include offenders who have a lot of money to spend on an expensive lifestyle. One of the cases focusing on banking malware, for example, includes offenders who spend more than two hundred thousand euros on luxury boats (case 155). Another case focuses on a criminal group involved in exchanging bitcoins for cash euros. Their customers are individuals who earned cryptocurrency through online drug transactions. Available information in the case files indicates the offenders are involved in several substantial expenditures, for example on cars and helicopter flights (case173). However, there are also cases in which the police found little or no evidence of substantial life style expenditures. Some cases even include offenders who seem to find it difficult to make a living (case 175, for example). In conclusion, regarding the consumption of criminal earnings, no major differences between traditional crime and cybercrime were found.

After consumption and reinvestment in criminal activities, an offender may have money left and may invest in legal economy. To analyse the investments of offenders, we checked all 30 cases of the fifth data sweep of the DOCM for available information on offenders' assets. When checking the case reports, we used every source of information available, i.e. we did not only look for confiscated assets but also used, among other sources, statements of suspects and witnesses, intelligence from informers, seized bookkeeping and records, and monitored telephone conversations. Earlier research showed that organized crime offenders predominantly invest in their country of origin or in their country of residence[4], which investments mainly consist of tangible, familiar assets such as residences, other real estate, and (mostly small) companies, which are often used for criminal activities. Offenders mainly invest in companies in well-known sectors, such as wholesale and retail, hotels and restaurants, and transport (Kruisbergen, Kleemans, and Kouwenberg 2015; see section 2). Regarding the investment of criminal proceeds (assets found), the analyses of our 30 cases show no major differences compared to these earlier findings. Furthermore, we found no major differences between traditional crime and cybercrime. Some cybercrime cases include offenders who are involved in IT-related companies, which is not often found in cases of traditional organized crime. However, this

actually fits pretty well within the general pattern described earlier; offenders' investments often are within their social and/or physical proximity.

In the next section, we focus on the laundering of criminal earnings. Money laundering is a basic necessity for offenders whose earnings exceed daily expenditures. Since our analyses on this topic did produce relevant differences between different types of cases, we will describe these results in more detail.

Laundering of criminal earnings

Criminal cash flows need to be kept out of sight. If offenders want to prevent getting apprehended and their money seized, criminal proceeds and/or the illegal origin, need to remain hidden. What role does IT play in this respect in the various cases?

When it comes to concealing criminal earnings, we do see important differences between traditional organized crime on the one hand and IT-related crime on the other. The 23 cases of traditional organized crime include various rudimentary money laundering arrangements as described in previous publications, such as the concealment and transfer of cash, and spending large amounts of cash, whether or not by using strawmen or facilitators, on (leasing) cars or renting real estate. We see the latter, for example, in a drug trafficking case. The main suspect spends € 20,000 in cash for the rent of a house in the Netherland, spends more than € 20,000 in cash on a Mercedes, spends many thousands of euros in cash for the purchase of (water) scooters, and lets a contact pay almost €9,000 in cash for a holiday trip (case 161). We also see more complex money laundering constructions, such as faking legal profit or salary, loan-back schemes, or the channelling of money through foreign legal entities (Kruisbergen, Van de Bunt, and Kleemans 2012).

In addition to the 'traditional' ways of money laundering, use can also be made of new payment methods enabled by IT, such as cryptocurrencies and prepaid cards. In principle, a cryptocurrency such as bitcoin is not only useful for cybercriminals. For example, criminals who are active in traditional, offline drug trafficking could use the purchase of bitcoins either in a construction to protect their money flows from detection or as a speculative investment. In the 23 cases of traditional organized crime, however, we do not see the use of bitcoins or other cryptocurrencies, although we do see the use of prepaid cards in one case (case 165). So, when it comes to money laundering, given the lack of financial innovation (except for the small-scale use of prepaid cards), the offenders in these 23 cases of traditional organized crime are still quite 'traditional'. The reasons for this could be that these offenders are unfamiliar with the new possibilities, they are afraid of the disadvantages of cryptocurrencies[5], they simply do not feel the need to change their modus operandi, or the police did not detect the use of virtual currencies.

In IT-related crime, unlike many forms of traditional organized crime, the proceeds are often digital in nature. People selling drugs on a dark web market often receive the proceeds of their merchandise in a cryptocurrency such as bitcoin. The perpetrators of phishing and malware attacks gain control over the online payment transactions of their victims, which take place in digital euros. Case 152 centres on online drugs and arms trade via a darknet market. Online drugs transactions are paid with bitcoins. During the police investigation, hundreds of bitcoins, worth roughly half a million euros, are seized during searches. One of the moderators of the online marketplace also sells narcotics himself. The police file states that the moderator/drug dealer has contacts where he can exchange bitcoins for physical euros. Apparently, he preferred to keep at least part of his earnings in cash. The exchange was done through individual bitcoin exchangers that were met in public places. There are various, easily accessible online bitcoin exchanges, but since they often require some form of identification, they are not attractive for a drug dealer. Because more online traders want to exchange their bitcoins for euros, the online trade in illegal goods has been accompanied by a demand for bitcoin exchange services that, as compared to regular channels, offer a higher degree of anonymity. Case 173 focuses on professional facilitators providing exactly this type of service. These facilitators also met their customers in public places.

The main suspects exchanged bitcoins for cash payments after being paid a commission. At least some of the bitcoins bought by them probably originate from illegal trade on the dark web. Indications supporting this conclusion are the following: the police find objects related to the shipment of drugs at customers of the bitcoin exchangers; a customer's bitcoin wallet can be connected to online drug trafficking; and customers have to pay a 7% commission, which is much higher than other, regular bitcoin exchangers.

The bitcoin exchangers meet their customers in local branches of hamburger or coffee chains (with Wi-Fi). After a customer has transferred bitcoins to a bitcoin wallet controlled by the exchanger, the customer receives the money in cash. For the exchangers, the large amount of bitcoins they obtain through this practice results in exchange and money laundering problems on their part. Part of the purchased bitcoins are exchanged for euros at regular bitcoin exchangers. The latter deposit the euros on accounts that are under the control of the exchangers. The money is withdrawn in cash and used again to purchase bitcoins. In total, the exchange service of the offenders amounts to millions of euros. (Case 173)

Cases 152 and 173, together with case 151, form part of the category of traditional organised crime with IT as an important innovative element. Case 154 and case 156 could be classified as organised low-tech cybercrime. In these cases, too, we see that digital currency, digital euros, is exchanged into physical currency, cash. In case 154, a somewhat older case, the offenders manipulate card readers from a large Dutch bank to read information from bank account holders. Through homemade debit cards, cash is then withdrawn in more than ten different countries, after which the money is transferred abroad, either by physical transportation or by money transfer services. Case 156 focuses on offenders who carry out phishing attacks. Money is transferred from a victim's account to the account of a so-called money mule. The money is then withdrawn in cash, either by the money mule or by a recruiter. In both cases of low-tech cybercrime (case 154, case 156), we do not see the use of cryptocurrencies, prepaid cards, or other innovations.

Cases 153 and 155 both focus on offenders involved in banking malware, something we have classified as organised high-tech cybercrime. The criminal group in case 153 infects computers and mobile phones with software to manipulate bank transactions. To hide their criminal earnings, the offenders use different methods.[6] Firstly, money from the victims' bank accounts is used to buy bitcoins, Web-money, and vouchers, among other things. The bitcoins are then (partly) exchanged for euros. A second cash flow consists of purchasing online goods, such as computers and telephones. Thirdly, money is transferred from the victims' accounts to accounts of money mules, after which it is withdrawn in cash. In case 155, offenders also use accounts of money mules to cash out the money. Moreover, these offenders also use part of the stolen money to buy bitcoins. In addition, a so-called bitcoin mixing service is used to conceal the link between the sending and receiving address of a bitcoin and thus protect the identity of (in this case) the recipient. In this case, more than € 300,000 cash is seized. These two cases of high-tech cybercrime (case 153 and 155) illustrate the use of 'new' payment methods, such as bitcoins. At the same time, however, these cases, too, highlight the importance of cash.

Cash is (still) king

The central role of cash is a predominant shared feature of the cases we studied, both in the field of traditional and IT-related organised crime. Criminals hide cash and make sure cash ends up in other countries. Furthermore, offenders of phishing and banking malware attacks use money mules to cash their digital euros. Likewise, criminals earning bitcoins from online drug trafficking exchange at least part of their cryptocurrency for cash euros (see also Custers, Pool, and Cornelisse 2018; Europol 2015; Soudijn 2018; Leukfeldt 2014; Leukfeldt, Kleemans, and Stol 2017a, 2017b, 2017c). Finally, offenders also buy expensive goods and services with cash.

With these cash flows, a wide range of service providers are used who either unconsciously, without asking a lot of questions, or quite deliberately, help offenders. For moving money, offenders can contact underground bankers or people who specialize in physical cash smuggling. Furthermore, offenders use bitcoin exchangers for discretely exchanging bitcoins for cash euros

earned through drug trafficking. The fact that these service providers are valuable is reflected in the price their customers are willing to pay. Soudijn and Reuter (2016) calculated the total costs of cash money smuggling for cocaine traders at 10% to 17% of the smuggled amount. The price customers have to pay for the services of the professional bitcoin exchangers, such as in case 173, seems to vary at for instance 7%, making it much more expensive than regular bitcoin exchangers. Furthermore, offenders in cases of phishing and banking malware use money mules for cashing out the stolen money. They operate more like straw men than as professional facilitators and have a rather replaceable position in the periphery of criminal networks. Research shows that they are mainly recruited among young adults from disadvantaged, urban areas (Custers, Pool, and Cornelisse 2018). Communication between perpetrators in case 155 (banking malware) shows that they are looking for money mules among persons who are easy to influence, such as, for example, (young) people with debts, psychological problems, or drug addiction. In our case material, we also see that money mules do not always receive the promised compensation (case 156 (phishing)).

In addition to moving and exchanging criminal earnings, accepting cash payments is also a kind of 'service' offenders utilize. In this fifth sweep, but also in previous reports of the DOCM, we see providers of goods and services in the regular economy accepting payment of (very) high amounts, seemingly without asking any questions (Kruisbergen, Van de Bunt, and Kleemans 2012). These facilitators, including car companies, providers of housing, electronics stores, contractors, travel agencies, and other providers of valuable goods and services, enable offenders to profit from criminal earnings.

Conclusion and discussion

In this final section we summarise the empirical results and highlight our contribution to the theoretical understanding of organised (cyber)crime. Furthermore, we examine methodological considerations of our study, and provide suggestions for future research.

Money laundering choices of organized crime offenders in a digital age

To gain insight into the money laundering choices of organized crime offenders, we analysed 30 large-scale criminal investigations into organized crime. These cases, which are part of the DOCM, cover types of offline organised crime, such as offline drug trafficking and human trafficking, as well as cases of cybercrime. The empirical analyses focused on spending of criminal earnings as well as laundering of those earnings.

Regarding the spending of criminal proceeds, in terms of both consumption and investment (assets found), the analyses show no major differences compared to previous research (that focused on traditional crime). Furthermore, we found several similarities and no major differences between cases of traditional organized crime and cybercrime cases. Investments mainly consist of tangible, familiar assets, such as residences and other real estate and (small) companies from well-known sectors.

When it comes to concealing criminal earnings, we do see important differences. IT-enabled features, such as cryptocurrencies and related (money laundering) services, are a major financial innovation. Cryptocurrencies offer a certain degree of anonymity and are the means of payment on dark web markets. Together with the TOR networks on which dark web markets operate, a currency such as bitcoin makes it possible for buyers and sellers of illegal goods and services to engage in more or less anonymous transactions. Cryptocurrencies, however, are also used in cases of predatory crime. In our cases, bitcoins were used in a case of online drug trafficking as well as in two cases of banking malware. In the cases of offline organized crime, however, offenders almost exclusively used traditional methods of money laundering. In these cases, we did not see any offender using cryptocurrencies, for example (although in one of the cases the criminals made use of another innovation, prepaid cards).

A striking similarity between cybercrime and traditional crime is the preference of offenders for cash. Malware and phishing offenders in our cases exchanged at least part of the stolen digital money for cash. Likewise, online drug traffickers sold (part of) the bitcoins they earned in exchange for cash euros (see also Europol, 2015; Custers, Pool, and Cornelisse 2018).

Our research adds to the theoretical understanding of how organized crime groups operate in the digital age in two ways. First, our analyses indicate that the operations of offenders involved in cybercrime are strongly dependent on resources in the offline world. The growth of the internet has opened up new horizons, for companies and consumers, but also for criminals. Physical and other boundaries need no longer pose an obstacle to any (legal or illegal) endeavour, at least in theory. However, despite the common notion of 'borderless crime', there is growing evidence that cybercrime has a significant local dimension and is embedded in the offline world. Offline social contacts turn out to play an important role in involvement mechanisms. Part of the members of cybercriminal networks know each other due to their network in the offline world and share, for example, the same local and/or social background (Leukfeldt, Kleemans, and Stol 2017a, 2017b, 2017c; Lusthaus and Varese 2017).[7] Our research adds to this understanding. The dominance of cash, too, shows that the distinction between cybercrime and traditional (organized) crime is not as clear-cut as some might assume. Moreover, the offenders' preference for cash euros is in itself one of the ingredients of the local dimension of cybercriminal operations. Receiving cash is a physical activity. In the case of exchanging cryptocurrencies, this activity took place by individual bitcoin exchangers using local facilities with wifi. In the case of cashing out the revenues of banking malware or phishing attacks, offenders often use money mules, who may be recruited in the local vicinity (see also Leukfeldt, Kleemans, and Stol 2017a; Custers, Pool, and Cornelisse 2018).

Second, our analyses included cases of cybercrime as well as cases of traditional, offline organized crime. Many studies either focus on cybercrime or on traditional organized crime. However, IT can have an important effect on traditional criminal operations as well. IT offers criminals new opportunities for communication and recruitment, for example, as is illustrated by the use of encryption technology and online meeting places (Bijlenga & Kleemans, 2018; Kruisbergen et al. 2018; Lavorgna 2013, 2015). In this perspective one could say that traditional organized crime is moving more and more to the online world (Lusthaus 2013; Broadhurst et al. 2014). Our article contributes to the scarce empirical research into this topic by focusing on the use of IT for handling criminal money flows, in both cybercrime cases and cases of traditional organized crime. As we concluded, IT-facilitated new payment methods were hardly used in the analysed cases of offline organized crime. Therefore, regarding methods to launder their cash earnings, traditional organized crime is still pretty 'traditional', at least in our cases (see also Soudijn 2018). This finding fits within the results of our analyses of investments of organized crime offenders in legal economy, as these 'investment portfolios' are in a sense rather conservative as well (see also Kruisbergen, Kleemans, and Kouwenberg 2015). One explanation might be that offenders tend to be conservative concerning financial decisions. Another might be that many criminals do not need to drastically change or innovate their working methods, simply because the traditional methods are sufficient. Finally, we don't want to rule out that the absence of (large-scale) financial innovation in these cases might also be the result of the data we used. In the analysed cases of traditional, offline organized crime, however, (large-scale) financial innovation seems to be absent.

Methodological considerations and directions for future research

Our research is based on analyses of 30, mainly large-scale, Dutch criminal investigations. Dutch police files contain the results of all methods of investigation deployed in a criminal investigation, such as wiretapping, monitoring of internet traffic, and undercover policing. A researcher who has access to police files benefits from these exclusive powers and gains equally exclusive insights into

the activities in which offenders participate. Police files are, therefore, a very rich source of information. Using police files, however, also has certain limitations. Research based on Dutch police files, by definition, only involves cases that were prioritized by the Dutch police and in which offenders were caught and prosecuted. As a result, it runs the risk that certain findings remain absent, not because the facts are not there, but simply because the police could not find them or because offenders were not prosecuted. Particularly in cases of cybercrime, law enforcement agencies may choose to disrupt criminal operations instead of (continuation of) a time-consuming, full-fledged criminal investigation and prosecution. It may be fruitful, therefore, to combine analyses of criminal investigations with analyses of information gathered during disruptive operations.

Since the last decades, organized crime control policies have become supplemented with a financial approach, i.e. financial investigation, the prevention of and fight against money laundering, and the confiscation of criminal earnings (see also Kruisbergen 2017). Relatively little is known, however, about the financial and economic choices offenders make during their criminal operations. Criminologists and researchers from other disciplines conducting empirical research in the field of (organized) crime, should incorporate a 'financial approach' as well, especially if the field of interest concerns cybercrime. Research on criminal money flows in cybercrime cases may benefit from the fact that part of the demand-supply interaction on online marketplaces is registered one way or the other. Analyses of data on online transactions, regarding drugs or online money laundering services (exchange services), for example, could produce valuable insights into price mechanisms and influential factors behind changes in price level. Furthermore, information on the distribution of criminal proceeds can reveal which criminals provide crucial services in criminal networks. A financial perspective, therefore, can teach us a lot about offenders and their behaviour.

Notes

1. We would like to thank Geralda Odinot, Maite Verhoeven, Ronald Pool, and Christianne de Poot for sharing five cases related to cybercrime (Odinot et al. 2017).
2. The numbers used to identify cases are the same as used in the research report (Kruisbergen et al. 2018). Since the five data sweeps of the DOCM resulted in 180 case reports, the numbers for cases analysed in the fifth data sweep run from 151 up to 180.
3. Following the work of Fijnaut et al. (1998, 26–27), organized crime is defined as crime committed by groups that primarily focus on illegal profit, systematically commit crimes that adversely affect society, and are fairly competent in shielding their activities from the authorities, in particular by being willing to use physical violence or eliminate individuals trough corruption. The Dutch Organized Crime Monitor uses a wide interpretation of shielding of activities. Besides (the threat of) violence and corruption, it includes the use of storefronts, communication in codes, counter-surveillance activities, and the misuse of experts, such as public notaries, public lawyers, and accountants. Because richness of information is an important criterion for selection, cases with a limited size and scope are not selected (see also Kleemans, Van den Berg, and Van de Bunt 1998, 22–23; Kruisbergen et al. 2018). Smaller cases of cybercrime were used in Leukfeldt, Kleemans, and Stol (2017a, 2017b, 2017c, 2017d).
4. To determine the location of the offender who owns the asset, we looked at de facto ownership of the asset. If, for example, information indicated that behind a person who has formal ownership rights another person is hidden who has actual control of an asset, we used the latter.
5. Such as the risk of theft of bitcoins that are stored via the internet, the limitations of the anonymity with which bitcoin transactions can be made (Meiklejohn et al. 2013; Ron and Shamir 2013; Custers, Pool, and Cornelisse 2018), the extremely volatile exchange rate, and the low usability of bitcoin for payments of regular goods and services in the offline world.
6. See also Custers, Pool, and Cornelisse (2018, 11), for a description of the modus operandi in this case.
7. Co-offenders, expertise, and tools are also found online (e.g. Soudijn and Zegers 2012).

Disclosure statement

No potential conflict of interest was reported by the authors.

Notes on contributors

E.W. Kruisbergen is researcher at the Research and Documentation Centre (WODC) of the Dutch Ministry of Justice and Security.

E.R. Leukfeldt is senior researcher cybercrime at the Netherlands Institute for the Study of Crime and Law Enforcement (NSCR) and director of the Cybersecurity and SMEs research group of the Hague University of Applied Sciences.

E.R. Kleemans is Full Professor (Serious and Organized Crime and Criminal Justice), VU School of Criminology, Faculty of Law, Vrije Universiteit Amsterdam, the Netherlands.

R.A. Roks is an Assistant Professor of Criminology at the Erasmus University of Rotterdam.

References

Barone, R., and D. Masciandaro. 2011. "Organized Crime, Money Laundering and Legal Economy: Theory and Simulations." *European Journal of Law and Economics* 32: 115–142. doi:10.1007/s10657-010-9203-x.

Bijlenga, N., and E. R. Kleemans. 2018. "Criminals Seeking ICT-expertise: An Exploratory Study of Dutch Cases." *European Journal of Criminal Policy and Research* 24 (3): 253–268. doi:10.1007/s10610-017-9356-z.

Broadhurst, R., P. Grabosky, M. Alazab, and S. Chon. 2014. "Organizations and Cyber Crime: An Analysis of the Nature of Groups Engaged in Cyber Crime." *International Journal of Cyber Criminology* 8 (1): 1–20.

Bruinsma, G. J. N. 1996. "Georganiseerde misdaad en legale economische sectoren [Organized Crime and Legal Economic Sectors]." In *De georganiseerde criminaliteit in Nederland* [Organized Crime in the Netherlands], edited by F. Bovenkerk, 125–132. Gouda: Quint.

Bulanova-Hristova, G., K. Kasper, G. Odinot, M. Verhoeven, R. Pool, C. de Poot, W. Werner, and L. Korsell, eds. 2016. *Cyber-OC - Scope and Manifestations in Selected EU Member States*. Wiesbaden: Bundeskriminalamt.

Cornish, D. B., and R. V. Clarke. 2002. "Analyzing Organized Crimes." In *Rational Choice and Criminal Behavior: Recent Research and Future Challenges*, edited by A. R. Piquero and S. G. Tibbetts, 41–64. New York: Garland.

Custers, B. H. M., R. L. D. Pool, and R. Cornelisse. 2018. "Banking Malware and the Laundering of Its Profits." *European Journal of Criminology*. doi:10.1177/1477370818788007.

Europol (European Police Office). 2015. *Why is Cash Still king? A Strategic Report on the Use of Cash by Criminal Groups as a Facilitator for Money Laundering*. Den Haag: European Police Office.

Fernández Steinko, A. 2012. "Financial Channels of Money Laundering in Spain." *British Journal of Criminology* 52 (5): 908–931. doi:10.1093/bjc/azs027.

Fijnaut, C. J. C. F., F. Bovenkerk, G. Bruinsma, and H. Van de Bunt. 1998. *Organized Crime in the Netherlands*. Boston: Kluwer Law International.

Kleemans, E. R., E. A. I. M. Van den Berg, and H. G. Van de Bunt. 1998. *Georganiseerde criminaliteit in Nederland: Rapportage op basis van de WODC-monitor* [Organized Crime in the Netherlands. Report of the WODC Monitor]. Den Haag: WODC.

Kleemans, E. R., M. E. I. Brienen, H. G. Van de Bunt, R. F. Kouwenberg, G. Paulides, and J. Barensen. 2002. *Georganiseerde criminaliteit in Nederland: Tweede rapportage op basis van de WODC-monitor* [Organized Crime in the Netherlands. Second Report of the Organized Crime Monitor]. Den Haag: WODC.

Kruisbergen, E. W. 2017. "Combating Organized Crime: A Study on Undercover Policing and the Follow-The-Money Strategy." PhD diss., Vrije Universiteit, Amsterdam.

Kruisbergen, E. W., E. R. Kleemans, and R. F. Kouwenberg. 2015. "Profitability, Power, or Proximity? Organized Crime Offenders Investing Their Money in Legal Economy." *European Journal on Criminal Policy and Research* 21 (2): 237–256. doi:10.1007/s10610-014-9263-5.

Kruisbergen, E. W., E. R. Leukfeldt, E. R. Kleemans, and R. A. Roks. 2018. *Georganiseerde criminaliteit en ICT Nederland. Rapportage in het kader van de vijfde ronde van de Monitor Georganiseerde Criminaliteit* [Organized Crime and IT. Report Based on the Fifth Round of the Organized Crime Monitor]. Den Haag: WODC.

Kruisbergen, E. W., H. G. Van de Bunt, and E. R. Kleemans. 2012. *Georganiseerde criminaliteit in Nederland. Vierde rapportage op basis van de Monitor Georganiseerde Criminaliteit* [Organized Crime in the Netherlands. Fourth Report of the Organized Crime Monitor]. Den Haag: Boom Lemma.

Lagazio, M., N. Sherif, and M. Cushman. 2014. "A Multi-level Approach to Understanding the Impact of Cyber Crime on the Financial Sector." *Computers & Security* 45: 58–74. doi:10.1016/j.cose.2014.05.006.

Lavorgna, A. 2013. "Transit Crimes in the Internet Age: How New Online Criminal Opportunities Affect the Organization of Offline Transit Crimes." Doctoral School of International Studies, University of Trento.

Lavorgna, A. 2015. "Organised Crime Goes Online: Realities and Challenges." *Journal of Money Laundering Control* 18 (2): 153–168. doi:10.1108/JMLC-10-2014-0035.

Leukfeldt, E. R. 2014. "Cybercrime and Social Ties: Phishing in Amsterdam." *Trends in Organized Crime* 17 (4): 231–249.

Leukfeldt, E. R., ed. 2017. *Research Agenda the Human Factor in Cybercrime and Cybersecurity*. Den Haag: Eleven International Publishing.

Leukfeldt, E. R., A. Lavorgna, and E. R. Kleemans. 2017d. "Organised Cybercrime or Cybercrime that Is Organised? an Assessment of the Conceptualisation of Financial Cybercrime as Organised Crime." *European Journal on Criminal Policy and Research* 23 (3): 287–300. doi:10.1007/s10610-016-9332-z.

Leukfeldt, E. R., E. R. Kleemans, and W. P. Stol. 2017a. "Cybercriminal Networks, Social Ties and Online Forums: Social Ties Versus Digital Ties within Phishing and Malware Networks." *British Journal of Criminology* 57 (3): 704–722.

Leukfeldt, E. R., E. R. Kleemans, and W. P. Stol. 2017b. "A Typology of Cybercriminal Networks: From Low-tech Locals to High-tech Specialists." *Crime, Law and Social Change* 67 (1): 21–37. doi:10.1007/s10611-016-9662-2.

Leukfeldt, E. R., E. R. Kleemans, and W. P. Stol. 2017c. "Origin, Growth and Criminal Capabilities of Cybercriminal Networks. An International Empirical Analysis." *Crime, Law and Social Change* 67 (1): 39–53. doi:10.1007/s10611-016-9663-1.

Levi, M., and P. Reuter. 2009. "Money Laundering." In *Handbook on Crime and Public Policy*, edited by M. Tonry, 356–380. New York: Oxford University Press.

Levi, M. 2012. "The Organization of Serious Crimes for Gain." In *The Oxford Handbook of Criminology*, edited by M. Maguire, R. Morgan, and R. Steiner, 595–622. 5th ed. Oxford: Oxford University Press.

Lusthaus, J. 2013. "How Organised Is Organised Cybercrime?" *Global Crime* 14 (1): 52–60. doi:10.1080/17440572.2012.759508.

Lusthaus, J., and F. Varese. 2017. "Offline and Local; the Hidden Face of Cybercrime." *Policing: A Journal of Policy and Practice*. Online first. doi:10.1093/police/pax042.

Malm, A., and G. Bichler. 2013. "Using Friends for Money: The Positional Importance of Money-launderers in Organized Crime." *Trends in Organized Crime* 16 (4): 365–381. doi:10.1007/s12117-013-9205-5.

Matrix Knowledge Group. 2007. "The Illicit Drug Trade in the United Kingdom." *Home Office Online Report 20/07*. London: Home Office. doi:10.1094/PDIS-91-4-0467B.

Meiklejohn, S., M. Pomarole, G. Jordan, K. Levchenko, D. McCoy, G. M. Voelker, and S. Savage. 2013. *A Fistful of Bitcoins: Characterizing Payments among Men with No Names*. San Diego: University of California.

Odinot, G., M. A. Verhoeven, R. L. D. Pool, and C. J. De Poot. 2017. *Organised Cybercrime in the Netherlands: Empirical Findings and Implications for Law Enforcement*. Den Haag: WODC. https://english.wodc.nl/

Petrunov, G. 2011. "Managing Money Acquired from Human Trafficking: Case Study of Sex Trafficking from Bulgaria to Western Europe." *Trends in Organized Crime* 14: 165–186. doi:10.1007/s12117-011-9127-z.

Przepiorka, W., L. Norbutas, and R. Corten. 2017. "Order without Law: Reputation Promotes Cooperation in a Cryptomarket for Illegal Drugs." *European Sociological Review* 33: 752–764. doi:10.1093/esr/jcx072.

Reuter, P. 2013. "Are Estimates of the Volume of Money Laundering either Feasible or Useful?" In *Research Handbook on Money Laundering*, edited by B. Unger and D. van der Linde, 224–231. Cheltenham: Edward Elgar.

Ron, D., and A. Shamir. 2013. "Quantitative Analysis of the Full Bitcoin Transaction Graph." *Financial Cryptography and Data Security* 7859: 6–24.

Schneider, F. 2010. "Turnover of Organized Crime and Money Laundering: Some Preliminary Empirical Findings." *Public Choice* 144: 473–486. doi:10.1007/s11127-010-9676-8.

Schneider, S. 2004. *Money Laundering in Canada: An Analysis of RCMP Cases*. Toronto, Canada: Nathanson Centre for the Study of Organized Crime and Corruption, York University.

Schuppers, K., N. Rombouts, P. Zinn, and H. Praamstra. 2016. *Cybercrime en ge-digitaliseerde criminaliteit: Nationaal dreigingsbeeld 2017* [Cybercrime and Digitised Crime: National Threat Assessment 2017]. Driebergen: Nationale Politie.

Soudijn, M. R. J. 2018. "Using Police Reports to Monitor Money Laundering Developments. Continuity and Change in 12 Years of Dutch Money Laundering Crime Pattern Analyses." *European Journal on Criminal Policy and Research*. doi:10.1007/s10610-018-9379-0.

Soudijn, M. R. J., and B. C. H. T. Zegers. 2012. "Cybercrime and Virtual Offender Conver-gence Settings." *Trends in Organized Crime* 15 (2–3): 111–129. doi:10.1007/s12117-012-9159-z.

Soudijn, M. R. J., and P. Reuter. 2016. "Cash and Carry: The High Cost of Currency Smuggling in the Drug Trade." *Crime, Law and Social Change* 66 (3): 271–290. doi:10.1007/s10611-016-9626-6.

Suendorf, U. 2001. *Geldwäsche: eine kriminologische Untersuchung* [Money Laundering: A Criminological Analysis]. Luchterhand: Neuwied und Kriftel.

Töttel, U., G. Bulanova-Hristova, and G. Flach, eds. 2016. *Research Conferences on Organised Crime at the Bundeskriminalamt in Germany, Volume III, Transnational Organised Crime, 2013–2015*. Wiesbaden: Bundeskriminalamt.

Transcrime. 2013. "Progetto PON sicurezza 2007–2013. Gli investimenti delle mafie [Mafia Investments]." *Summary*. www.investimentioc.it

Unger, B., M. Siegel, J. Ferwerda, W. De Kruijf, M. Busuioic, K. Wokke, and G. Rawlings. 2006. *The Amounts and the Effects of Money Laundering. Report for the Ministry of Finance, February 16, 2006*. Utrecht: Utrecht School of Economics; Canberra, Australia: Australian National University.

Van Duyne, P., and M. Levi. 2005. *Drugs and Money. Managing the Drug Trade and Crime-Money in Europe*. Abingdon: Routledge.

Van Duyne, P. C. 2003. "Money Laundering Policy. Fears and Facts." In *Criminal Finances and Organising Crime in Europe*, edited by P. C. Van Duyne, K. Von Lampe, and J. L. Newell, 67–104. Nijmegen: Wolf Legal Publishers.

Van Duyne, P. C., and M. R. J. Soudijn. 2010. "Crime-Money in the Financial System: What We Fear and What We Know." In *Transnational Criminology Manual*, edited by M. Herzog-Evans, 253–279. Nijmegen: Wolf Legal.

Verhage, A. 2011. *The anti-Money Laundering Complex and the Compliance Industry*. Abingdon: Routledge.

Walker, J. 1995. "Estimates of the Extent of Money Laundering in and through Australia." Paper prepared for the Australian Transaction Reports and Analysis Centre, Queanbeyan, Australia: John Walker Consulting Services.

Webb, S., and J. Burrows. 2009. "Organised Immigration Crime: A Post-conviction Study." *Home Office Research Report 15*. London: Home office.

Werner, Y., and L. Korsell. 2016. "Cyber-OC in Sweden." In *Cyber-OC: Scope and Manifestations in Selected EU Member States*, edited by G. Bulanova-Hristova, K. Kasper, G. Odinot, M. Verhoeven, R. Pool, C. de Poot, W. Werner, and L. Korsell, 101–164. Wiesbaden: Bundeskriminalamt.